AMENDED IN ASSEMBLY MAY 8, 2008

AMENDED IN ASSEMBLY APRIL 22, 2008

AMENDED IN ASSEMBLY APRIL 3, 2008

CALIFORNIA LEGISLATURE—2007–08 REGULAR SESSION

ASSEMBLY BILL No. 2362

Introduced by Assembly Member Keene

February 21, 2008

An act to amend Section 1798.29 of the Civil Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

AB 2362, as amended, Keene. State records: personal information: security breaches.

~~(1) Existing~~

Existing law, the Information Practices Act of 1977, requires any agency that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways any breach of security of the data, as defined, to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law authorizes an agency to provide that disclosure by written notice, by electronic notice, or, upon a specified condition, by substitute notice.

This bill would require an agency, when collecting personal information from a resident to provide notice to the resident that his or her personal information is being handled in a secure manner that guards against unauthorized disclosure and, in the event of a breach of the security of the system, to provide timely and appropriate notice. ~~By adding to the procedures local agencies must follow when collecting~~

~~personal information, this bill would impose a state-mandated local program.~~

~~(2) The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.~~

~~This bill would provide that, if the Commission on State Mandates determines that the bill contains costs mandated by the state, reimbursement for those costs shall be made pursuant to these statutory provisions.~~

~~(3) This~~

This bill would make the operation of its provisions contingent upon the enactment of AB 1779 of the 2007–08 Regular Session.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: ~~yes~~ *no*.

The people of the State of California do enact as follows:

SECTION 1. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this

section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4) Medical information.

(5) Health insurance information.

(f) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(i) ~~When~~ *Consistent with subdivision (j), when* collecting personal information from a resident of this state, an agency shall provide notice to the resident that his or her personal information is being handled in a secure manner that guards against unauthorized disclosure and that in the event of a breach of the security of the system, timely and appropriate notice shall be provided.

(j) To the extent agencies provide the notice required in subdivision (i) by incorporating the notice into existing forms and documents, the notice may be incorporated as part of the agency's earliest scheduled revisions to those forms and documents occurring on or after January 1, 2009.

~~SEC. 2. If the Commission on State Mandates determines that this act contains costs mandated by the state, reimbursement to local agencies and school districts for those costs shall be made pursuant to Part 7 (commencing with Section 17500) of Division 4 of Title 2 of the Government Code.~~

~~SEC. 3.~~

SEC. 2. This act shall become operative only if Assembly Bill 1779 of the 2007–08 Regular Session is enacted and becomes effective on or before January 1, 2008.

O